CONFIDENCIAL

FINTRIXS PAY

Ciberseguridad y seguridad de la información

04.5 — CONTROLES TÉCNICOS EN PASARELA DE PAGOS PROPIA (VENTA NO PRESENTE)

CÓDIGO	CIB-005
VERSIÓN	1.0 — 16 de abril de 2026
APROBADO POR	Representante Legal
VIGENCIA	—

FINTRIXS S.A.S. · NIT 901.994.194-3
Paquete de Due Diligence — Banco Sponsor Agregador
Emitido el 16 de abril de 2026 — Versión 1.0 del paquete

04.5 — CONTROLES TÉCNICOS EN PASARELA DE PAGOS PROPIA (VENTA NO PRESENTE) · Código: CIB-005 · Versión: 1.0 — 16 de abril de 2026 · FINTRIXS S.A.S.

1. Vista general

Fintrixs Pay es una pasarela propia operada sobre microservicios. A continuación se detalla el mapeo entre las prácticas solicitadas por el banco y su implementación concreta.

2. Tabla de controles

Control solicitado por el DD	Implementación en Fintrixs Pay
Control de acceso y autenticación (MFA, RBAC, OAuth, JWT, mTLS)	JWT RS256 en todas las APIs (`auth-service`). MFA obligatoria para administradores y operaciones críticas. RBAC + ABAC. OAuth 2.0 / OpenID Connect para integraciones. mTLS en comunicaciones entre microservicios.
Validaciones de entrada y sanitización de datos	DTOs obligatorios con `class-validator` en todos los endpoints NestJS. Validación en gateway (Kong plugins) y en la capa de servicio.
Gestión de sesiones	JWT de corta vida + refresh tokens con rotación. Revocación por lista negra. TTL configurado por tipo de cliente.
Protección contra ataques comunes (XSS, CSRF, Fuerza bruta)	CSP estricto, sanitización automática, anti-CSRF tokens, rate limiting en Kong, captcha adaptativo, bloqueo progresivo.
Cifrado y protección de datos (tránsito y reposo)	TLS 1.2+ (pref. 1.3) en todos los endpoints. AES-256 en reposo. Tokenización para PAN. KMS gestionado.
Gestión de logs y monitoreo	`@fintrixs/logging` — logs estructurados PCI-safe con masking automático, centralizados en SIEM. Retención de 5 años.
Actualizaciones y parches	Pipeline CI/CD con imágenes base actualizadas semanalmente, `trivy` y `dependabot` para CVEs.
Gestión de claves y credenciales	Secret manager centralizado (KMS + vault). Prohibido almacenar credenciales en código o env planos. Rotación periódica.
Cifrado y validación de certificados	Validación de CA raíz en mTLS. Pinning en aplicaciones móviles.
Copias de seguridad y recuperación	Backups cifrados diarios + incrementales cada 15 min. Retención por política. Restore probado trimestralmente.
Aislamiento y segmentación (Zero Trust)	CDE (Cardholder Data Environment) segmentado lógicamente. Políticas NetworkPolicy en Kubernetes. No confía en la red, cada servicio verifica identidad.
Seguridad en APIs (versionamiento, headers, API Gateway)	Kong 3.5 como API Gateway: rate limiting, transformación, autenticación, WAF plugins. Versionamiento semántico. Headers de seguridad.
Configuración segura del servidor	Hardening CIS Benchmarks, imágenes Distroless / Chainguard. Usuarios no privilegiados. AppArmor / SecComp.
Prevención de inyección de código (SQLi, XSS)	ORM parametrizado (TypeORM). Validación estricta. Headers CSP. SAST en CI.

Control solicitado por el DD	Implementación en Fintrixs Pay
Prevención CSRF	Tokens anti-CSRF en cookies SameSite.
Protección DDoS/DoS	AWS Shield + CloudFront + rate limiting en Kong + alertas.
Protección clickjacking	Headers `X-Frame-Options: DENY` y CSP frame-ancestors.
Fuerza bruta y enumeración de usuarios	Respuestas uniformes, bloqueo progresivo, captcha, MFA.
Legitimidad de comunicaciones front-back	JWT + CSRF + validación de origen + mTLS interno.
Gestión de sesiones y validación de tokens	TTL cortos, revocación, tokens firmados RS256, auditoría.
Validaciones de entrada	`class-validator`, schemas de Kafka, validación en gateway.
Control de acceso (RBAC)	Roles definidos, `@fintrixs/authz` guard en cada endpoint sensible.
Cifrado de datos sensibles en reposo	AES-256 para PII y datos financieros. KMS.
Logging y monitoreo	SIEM centralizado. Alertas por anomalías. Correlación de eventos.

3. Controles específicos PCI DSS v4.0

Los controles están detallados y evidenciados en `docs/pci-dss/`. Mapeo resumido:

Requisito PCI DSS	Implementación en Fintrixs Pay
1. Firewall / segmentación	Kong + AWS Security Groups + NetworkPolicies
2. Hardening	CIS Benchmarks + pipelines
3. Protección de datos almacenados (PAN)	Tokenización + vault cifrado, nunca se persiste PAN/CVV fuera del vault
4. Cifrado en tránsito	TLS 1.3 preferente, mTLS entre servicios
5. Antimalware	EDR en endpoints y servidores administrativos
6. Secure SDLC	OWASP ASVS, SAST/DAST, revisión de código
7. Restricción de acceso	RBAC + mínimo privilegio
8. Identificación y autenticación	MFA + JWT RS256 + rotación
9. Acceso físico	Hosting en AWS (SOC 2 / PCI DSS)
10. Logs y monitoreo	`@fintrixs/logging` + SIEM + retención
11. Pruebas de seguridad	ASV + pentest + SAST/DAST
12. Política y respuesta a incidentes	SGSI + CSIRT

4. 3D Secure y tokenización

- **3DS 2.2** a través de la red adquirente Credibanco para transacciones de venta no presente.
- **Tokenización de tarjeta** gestionada por Credibanco + tokens internos de Fintrixs (`tokenization-service`) que reemplazan el PAN en toda la plataforma.

5. Datos que Fintrixs no persiste

- **CVV/CVC2:** nunca se almacena (PCI DSS Req. 3.3).
- **PIN / PIN block:** nunca.
- **Track data / banda magnética:** nunca.
- **PAN en claro fuera del vault:** nunca; el resto de servicios trabaja exclusivamente con tokens.